What is claimed is:

1. A method of securely configuring a first machine in a pre-operating system environment, the method comprising:

determining an operating mode of the machine; providing an attestation;

performing a shared secret key exchange; receiving a configuration update; and

detecting a message;

updating a machine configuration in a pre-operating system

environment.

- 2. A method as defined in claim 1, wherein the message is sent from a second machine.
- 3. A method as defined in claim 1, wherein the operating mode of the first machine comprises at least one of an IT-managed machine and a consumer machine.
- 4. A method as defined in claim 1, wherein the attestation comprises at least one of machine identity information and a pseudo-anonymous authentication.
- 5. A method as defined in claim 4, wherein the pseudo-anonymous authentication is provided by a trusted platform module.

- 6. A method as defined in claim 4, wherein the machine identity information comprises at least one of a serial number, a network name, and a cryptographic representation of hardware registers.
- 7. A method as defined in claim 4, wherein the pseudo-anonymous authentication comprises an Attestation Identity Key.
- 8. A method as defined in claim 1, wherein updating the machine configuration in a pre-operating system environment is adapted to operate in an OS-transparent operating mode with networking support.
- 9. A method of securely configuring a client operating in a pre-operating system environment, the method comprising:

sending a message;

determining an operating mode of the client machine;

receiving an attestation;

verifying the attestation;

performing a shared secret key exchange; and

sending a configuration update to the client machine in a pre-operating

system environment.

10. A method as defined in claim 9, wherein the message is to a client machine.

- 11. A method as defined in claim 9, wherein the operating mode of the client machine comprises at least one of an IT-managed device and a personal device.
- 12. A method as defined in claim 9, wherein the attestation comprises at least one of client machine identity information and a pseudo-anonymous authentication.
- 13. A method as defined in claim 12, wherein the client machine identity information comprises at least one of a serial number, a network name, and a cryptographic representation of hardware registers.
- 14. A method as defined in claim 12, wherein the pseudo-anonymous authentication comprises an Attestation Identity Key.
- 15. A method as defined in claim 9, wherein the attestation is verified by a trusted third party.
- 16. A method as defined in claim 9, wherein the configuration comprises at least one of a firmware setting, a BIOS setting, and a machine setting.
- 17. A method as defined in claim 16, wherein the configuration update comprises an encrypted configuration update.

- 18. A method as defined in claim 9, wherein sending the configuration update to the client machine in a pre-operating system environment is adapted to operate in an OS-transparent operating mode with networking support.
- 19. An apparatus to securely configure a client machine in a pre-operating system environment, the apparatus comprising:

a client machine comprising:

a messaging module configured to detect messages and send messages;

an operating mode;

a trusted platform module configured to provide an attestation;

a key exchange module configured to perform a shared secret

key exchange; and

a configuration module configured to update the client's configuration in a pre-operating system environment; and

a server machine comprising:

an messaging module configured to send messages and receive messages;

a key exchange module configured to perform a shared secret key exchange after an attestation has been verified; and

an update module configured to generate a client configuration update.

- 20. An apparatus as defined in claim 19, wherein the client machine's operating mode comprises at least one of an IT-managed machine and a consumer machine.
- 21. An apparatus as defined in claim 19, wherein the trusted platform module is configured to use at least one of a pseudo-anonymous authentication and machine identity information.
- 22. An apparatus as defined in claim 19, wherein the configuration module is configured to update at least one of a firmware setting, a BIOS setting, and a machine setting.
- 23. An apparatus as defined in claim 19, wherein the configuration module is adapted to update the client's configuration in an OS-transparent operating mode with networking support.
- 24. An apparatus as defined in claim 19, wherein the update module is configured to generate at least one of a firmware update, a BIOS update, and a machine setting update.
- 25. An apparatus as defined in claim 19, wherein the server machine further comprises an encryption module configured to encrypt the client configuration update.

26. A machine readable medium having instructions stored thereon that, when executed, cause a machine to:

detect a message;

determine an operating mode of the machine;

provide an attestation;

perform a shared secret key exchange;

receive a configuration update; and

update a machine configuration in a pre-operating system environment.

- 27. A machine readable medium as defined in claim 26, having instructions stored thereon that, when executed, cause the machine to receive the message from a server.
- 28. A machine readable medium as defined in claim 26, having instructions stored thereon that, when executed, cause the machine to update at least one of a firmware setting, a BIOS setting, and a machine setting.
- 29. A machine readable medium having instructions stored thereon that, when executed, cause a first machine to:

send a message;

determine an operating mode of a second;

receive an attestation;

verify the attestation;

perform a shared secret key exchange; and

send a configuration update to the client machine in a pre-operating system environment.

- 30. A machine readable medium as defined in claim 29, having instructions stored thereon that, when executed, cause the first machine to send the message via a network connection.
- 31. A machine readable medium as defined in claim 29, having instructions stored thereon that, when executed, cause the first machine to query a trusted third party to verify the attestation.
- 32. A machine readable medium as defined in claim 29, having instructions stored thereon that, when executed, cause the first machine to encrypt the configuration update.